PATENT ABSTRACTS OF JAPAN

(11)Publication number : **03-263147**
(43)Date of publication of application : **22.11.1991**

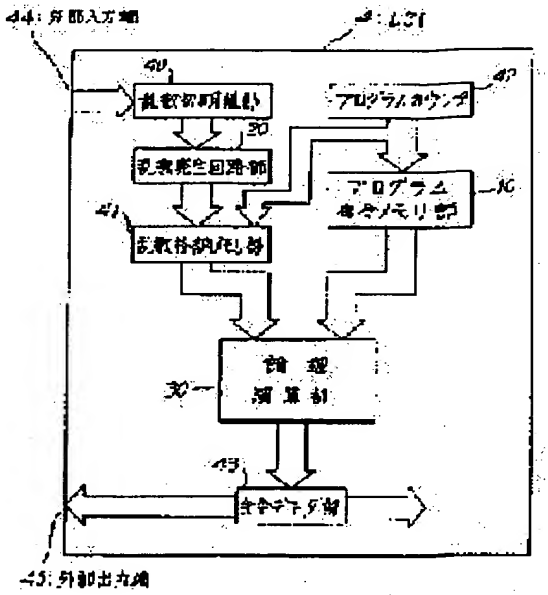
(51)Int.Cl. **G06F 12/14**
G06F 9/06

(21)Application number : **02-062060**
(22)Date of filing : **13.03.1990**

(71)Applicant : **FUJITSU LTD**
(72)Inventor : **MAEDA TOKUNORI**

(54) SEMICONDUCTOR INTEGRATED CIRCUIT DEVICE

(57)Abstract:
PURPOSE: To execute the data output whose decoding is difficult by generating irregular data by executing the data conversion of store data by random number data generated by a random number generating circuit part, and executing the encipherment thereof.
CONSTITUTION: An LSI (Large scale integrated circuit device) 4 is provided with a program instruction memory part 10, a random number initial value part 40, a random number generating circuit part 20, a random number store memory part 41, and a logical arithmetic part 30, and to the program instruction memory part 10, a program counter 42 is connected, and an output terminal of the logical arithmetic part 30 is connected to an instruction decoder part 43. In such a state, random number data of an intrinsic pattern related in advance to a certain initial value is generated, and store data is converted to data having irregularity being different from that of the store data by this random number data. In such a way, the LSI having a data enciphering circuit whose decoding is difficult is obtained.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's

⑲日本国特許庁(JP)　⑪特許出願公開

⑫公開特許公報(A)　平3−263147

⑤1Int.Cl.⁵	識別記号	庁内整理番号
G 06 F 12/14	320 B	7165−5B
9/06	450 B	7927−5B

⑬公開　平成3年(1991)11月22日

審査請求　未請求　請求項の数 5　(全5頁)

⑤4発明の名称　半導体集積回路装置

⑳特　願　平2−62060
㉒出　願　平2(1990)3月13日

⑦2発明者　前田　徳則　神奈川県川崎市中原区上小田中1015番地　富士通株式会社内
⑦1出願人　富士通株式会社　神奈川県川崎市中原区上小田中1015番地
⑦4代理人　弁理士　石川　泰男

明　細　書

1．発明の名称

半導体集積回路装置

2．特許請求の範囲

1．格納データを読み出し可能なメモリ手段(1、10)と、ある初期値に対して予め関連づけられた固有のパターンの乱数データを発生する乱数発生手段(2、20)と、

前記格納データを前記乱数データにより前記格納データとは異なる不規則性を有するデータに変換するデータ変換手段(3、30)とを備えたことを特徴とする半導体集積回路装置。

2．前記格納データは、前記半導体集積装置において用いるプログラム命令データであることを特徴とする請求項1記載の半導体集積回路装置。

3．前記格納データは、前記乱数発生手段(2、20)が特定の初期値に基づいて発生する固有パターンの乱数データが前記データ変換手段(3、30)に与えられた場合にのみ正常なデータとなるように予め変換されていることを特徴とする請求項1又は2記載の半導体集積回路装置。

4．前記格納データは、前記半導体集積回路装置の外部に導出される場合にのみ前記データ変換手段(3、30)を経由することを特徴とする請求項1又は2記載の半導体集積回路装置。

5．前記データ変換手段(3、30)は、排他的論理和回路であることを特徴とする請求項1、2、3又は4記載の半導体集積回路装置。

3．発明の詳細な説明

〔概要〕

半導体集積回路装置(以下、LSIという。)に係り、より詳しくは、プログラム命令メモリ等のデータを内蔵するLSIに関し、

より解読困難なデータ暗号化回路を有する半導体集積回路装置を提供することを目的とし、

請求項1記載の発明は、格納データを読み出し

可能なメモリ手段と、ある初期値に対して予め関連づけられた固有のパターンの乱数データを発生する乱数発生手段と、前記格納データを前記乱数データにより前記格納データとは異なる不規則性を有するデータに変換するデータ変換手段とを備えて半導体集積回路装置を構成する。

〔産業上の利用分野〕

本発明は、半導体集積回路装置（以下、ＬＳＩという。）に係り、より詳しくは、プログラム命令メモリ等のデータを内蔵するＬＳＩに関する。

シングルチップ化されたマイクロコンピュータやＤＳＰ（ディジタル・シグナル・プロセッサ）などには、内部にＲＯＭ（読み出し専用メモリ：Read Only Memory）等のプログラム命令メモリが内蔵されている。この場合、ＬＳＩの信頼性向上の為、プログラム命令メモリの内容を外部に出力できるような構成になっている。このため第三者にもプログラム命令メモリの内容を見ることが可能であり不都合である。

〔従来の技術〕

従来のプログラム内容保護回路としては、アドレス又はデータをインバータなどの論理回路によって変更することによって暗号化するものや、アドレスのスクランブルによってプログラムの流れを暗号化するものがあった。

〔発明が解決しようとする課題〕

しかし、上記従来の技術では、暗号化されたデータが比較的簡単な規則に従った内容となり、複雑な加工を施したとしても解読は可能であった。

本発明の目的は、より解読困難なプログラムデータ暗号化回路を有する半導体集積回路装置を提供することにある。

〔課題を解決するための手段〕

第１図に、請求項１にかかる発明の原理説明図を示す。

上記課題を解決するために、請求項１記載の発明は、格納データを読み出し可能なメモリ手段（１）と、ある初期値に対して予め関連づけられた固有のパターンの乱数データを発生する乱数発生手段（２）と、前記格納データを前記乱数データにより前記格納データとは異なる不規則性を有するデータに変換するデータ変換手段（３）とを備えて半導体集積回路装置を構成する。

〔作用〕

上記構成を有する請求項１記載の発明にかかる半導体集積回路装置によれば、乱数発生回路部の発生する乱数データにより、格納データをデータ変換することによって不規則なデータを生成し、暗号化をおこなう。したがって、従来の暗号化回路を含む半導体集積回路装置に比べ、より解読困難なデータ出力を行うことができる。

〔実施例〕

第１実施例

第２図に請求項１、２、３、５記載の発明の実施例である第１実施例を示す。このＬＳＩ４は、メモリ手段であるプログラム命令メモリ部１０と、乱数初期値部４０と、乱数発生手段である乱数発生回路部２０と、乱数格納メモリ部４１と、データ変換手段である論理演算部３０とを備えている。プログラム命令メモリ部１０には、プログラムカウンタ４２が接続されている。また、論理演算部３０の出力端は、命令デコーダ部４３に接続されている。プログラム命令メモリ部１０は、このＬＳＩ４の格納データであるプログラム命令データを格納するＲＯＭである。乱数初期値部４０は、乱数の初期値を発生する。乱数発生回路部２０は、乱数初期値部４０から与えられる初期値に基づき乱数データを発生する。この場合、乱数発生回路部２０は、初期値が同一であれば、予め関連づけられた固有のパターンの乱数データを発生するような回路である。

乱数格納メモリ部４１は、乱数発生回路部２０が発生した乱数データを格納するＲＡＭ（Random Access Memory）であり、プログラム命令メモリ部１０とプログラムカウンタ４２によって同期し

ている。すなわち、プログラム実行時に乱数格納メモリ部４１の内容によって正規化するため、プログラム命令メモリ部１０と乱数格納メモリ部４１は、アドレス数が同じで各アドレスは同一ワード数となっている。論理演算部３０は、排他的論理和（エクスクルーシブＯＲ）回路を備え、プログラム命令メモリ部１０の出力データと、乱数格納メモリ部４１の出力データとの排他的論理和を演算し、その出力を命令デコーダ部４３に供給する。

次に、第４図に、第１実施例のＬＳＩの動作を説明する。プログラム命令データを、仮に、第４図のように４ワードデータとする。また、乱数発生回路部２０が発生し乱数格納メモリ部４１が格納する乱数データは、プログラム命令データに対応する形となっている。

図示例の場合、論理演算部３０にある特定の解読用乱数データＡが与えられた時のみ、プログラム命令データＢは正しいプログラム命令Ｃとして出力される。排他的論理和の真理値は図示の通りである。

すなわち、プログラム命令データＢは、所定の解読用乱数データＡが与えられたときにのみ、正しいプログラム命令Ｃとなるように予め変換され記憶されている。従って、第２図に示すＬＳＩの外部入力端４４に初期値を入れて外部出力端４５からプログラム内容を読み出そうとしても、解読用乱数データＡを発生させるような特定の初期値でない限り、正しいプログラム命令Ｃを読み出すことはできない。また、何らかの方法でＲＯＭの内容を直接読み出してもプログラム命令データＢは、正しいプログラム命令Ｃとは全く異なっており、この場合もプログラム内容を読み出すことはできない。

この第１実施例において、プログラム命令メモリ部１０は、ＲＯＭに限らず他のタイプのメモリであってもよく、格納データは、プログラム命令データには限定されず、このＬＳＩ４において用いる他のデータであってもかまわない。

また、乱数初期値は、乱数初期値部４０を介さず、ＬＳＩ４の内部又は外部から直接与えてもよい。

さらに、乱数格納メモリ部４１は省略して、プログラム命令メモリ部のデータ出力時にあわせて、乱数発生回路部２０から論理演算部３０に、直接、乱数データを出力してもよい。

また、上記の論理演算は、排他的論理和には限られない。排他的論理和は、第４図の真理値表に示すように、一方の入力Ｉが０の場合は、他の入力Ⅱをそのまま排他的論理和出力Ｘとして出力し、また、入力Ｉが１の場合には入力Ⅱを反転して出力するところに特徴があり、論理としてはかなり複雑である。

しかし、請求項１記載の発明によれば、特定の初期値のときのみ固有の乱数パターンを発生し、その場合に限って論理演算により正しいプログラム内容を出力するようにＲＯＭ内のプログラム内容Ｂをあらかじめ変換しておけばよい。

したがって、論理演算部３０としては、否定（ＮＯＴ）、論理積（ＡＮＤ）、論理和（ＯＲ）又は負論理（ＮＡＮＤ、ＮＯＲ）、さらには、これら論理の組合せでもかまわない。

第２実施例

次に、第３図に請求項１、２、４、５記載の発明の実施例である第２実施例を示す。

第２実施例のＬＳＩ４は、第１実施例と同様に、メモリ手段であるプログラム命令メモリ部１０と、乱数初期値部４０と、乱数発生手段である乱数発生回路部２０と、乱数格納メモリ部４１と、データ変換手段である論理演算部３０とを備えている。プログラム命令メモリ部１０には、プログラムカウンタ４２が接続されている。論理演算部３０は、排他的論理和回路を備えている。第２実施例が第１実施例と異なる点は、プログラム命令メモリ部１０のプログラム命令データを外部出力端４５に出力する場合のみ論理演算部３０を経由する点である。ＬＳＩ内においては、プログラム命令メモリ部１０から命令デコーダ部４３にそのまま出力される。

したがって、この場合には、プログラム命令メ

モリ部１０のプログラム命令データは予め変換は施されていない。このため、ＬＳＩの出力端４５からプログラム内容を読み出そうとする場合には、論理演算部３０に特定の解読用乱数データＡを与えない限り、第１実施例と同様に、全く規則性のないデータとして出力される。ただし、何らかの方法でプログラム命令メモリ部１０の内容を直接読み出せば、正しいプログラム内容が読み出せることになる。しかし、第１実施例のようにプログラム命令メモリ部の内容を予め変換しておく必要がなく取扱いが簡便であるという利点を有する。

第２実施例の場合も、プログラム命令メモリ部１０はＲＯＭに限られず、格納データはプログラム命令データには限定されない。また、乱数初期値部を介さず、ＬＳＩの内部又は外部から直接初期値を与えてもい。さらに、乱数格納メモリ部４１を介さず乱数データを直接論理演算部３０に出力してもよい。そして論理演算部３０の論理として、排他的論理和のみならず、他の論理を用いることが可能である。

〔発明の効果〕

以上説明した様に、請求項１記載の発明によれば、暗号化の種類も多くその規則性も判別しにくいという効果を奏し、プログラム内容の保護に寄与するところが大きいという利点を有する。

４．図面の簡単な説明

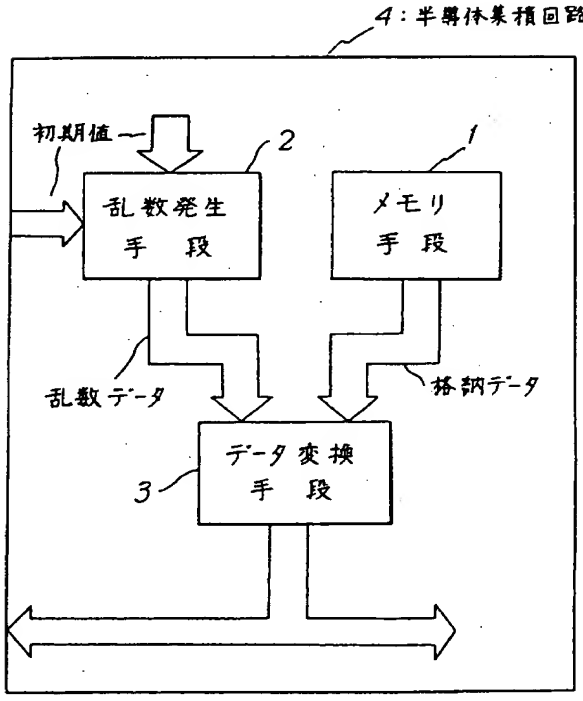
第１図は、請求項１記載の発明の原理説明図、

第２図は、請求項１、２、３又は５記載の発明の第１実施例の構成を示すブロック図、

第３図は、請求項１、２、４又は５記載の発明の第２実施例の構成を示すブロック図、

第４図は、第１実施例のＬＳＩの発明の動作を説明する図である。

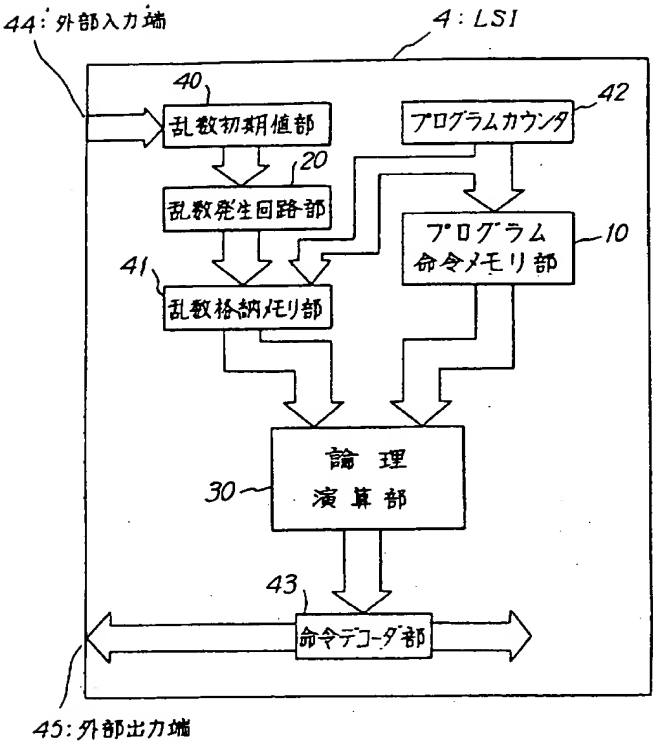
１…メモリ手段
２…乱数発生手段
３…データ変換手段
４…ＬＳＩ
１０…プログラム命令メモリ部
２０…乱数発生回路部
３０…論理演算部
４０…乱数初期値部
４１…乱数データ格納メモリ部
４２…プログラムカウンタ
４３…命令デコーダ
４４…外部入力端
４５…外部出力端
Ａ…解読用乱数データ
Ｂ…プログラム命令データ
Ｃ…正しいプログラム命令
Ｘ…排他的論理和出力



請求項1記載の発明の原理説明図

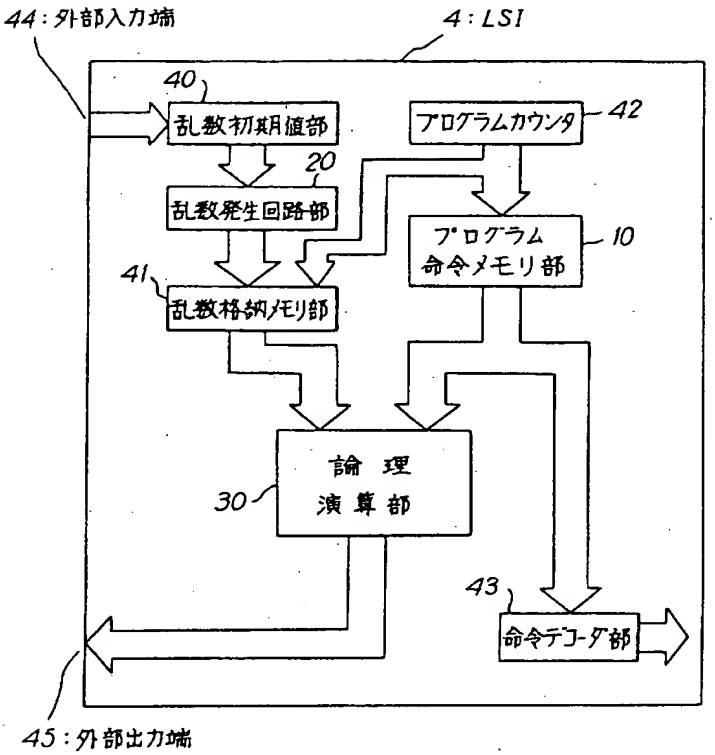
第１図

出願人代理人　石　川　泰　男



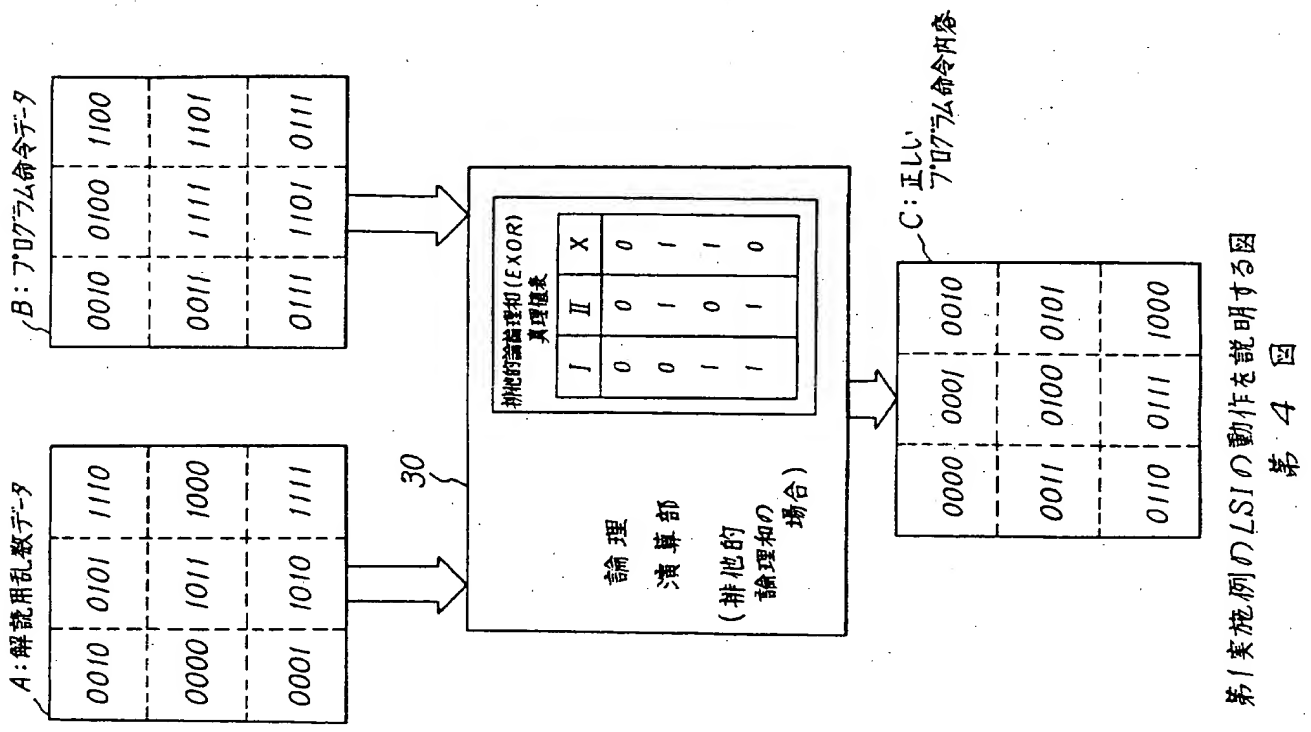
請求項1、2、3、5記載の発明の
第1実施例の構成を示すブロック図

第 2 図



請求項1、2、4、5記載の発明の
第2実施例の構成を示すブロック図

第 3 図



第1実施例のLSIの動作を説明する図

第 4 図